Práctica: Hash de un fichero

Objetivo: Realizar un Hash MD5 de un fichero, comprobar las colisiones y sustituir los hash por SHA-1

Desarrollo:

1. Crear un nuevo proyecto de consola
2. Implementa una función para realizar el Hash MD5 de un fichero

```
private String hashMD5(String file) throws Exception {
        MessageDigest md = MessageDigest.getInstance("MD5");
        BufferedInputStream in = new BufferedInputStream(new FileInputStream(     file));

        int theByte = 0;
        while ((theByte = in.read()) != -1) {
                md.update((byte) theByte);
        }
        in.close();

        byte[] theDigest = md.digest();
        return getHex(theDigest);
}
```

2.1. Función auxiliar para convertir un array de bytes en hexadecimal

```
final String HEXES = "0123456789ABCDEF";

private String getHex(byte[] raw) {
        if (raw == null) {
                return null;
        }
        final StringBuilder hex = new StringBuilder(2 * raw.length);
        for (final byte b : raw) {
                hex.append(HEXES.charAt((b & 0xF0) >> 4)).append(
                                HEXES.charAt((b & 0x0F)));
        }
        return hex.toString();
}
```

3. Ejecutar el programa para genera el hash de los fichero "Barack Obama.pdf" y "Paris Hilton.pdf". ¿Qué sucede?

4. Cambia el algoritmo por SHA-1, compara los resultados

Web: www.sidertia.com
Email: info@sidertia.com
Tel: 646.366.781 | 646.116.305
Centro de Empresas Carabanchel
C/ Cidro, 3 - Oficina 207 28044 MADRID